

RELEASE 1.0

6-96

ESTHER DYSON'S MONTHLY REPORT

19 JUNE 1996

LAW AND BORDERS

by David R. Johnson and David G. Post

As writers and thinkers, we always build (to put it politely) on the work of others. Sometimes we incorporate their ideas into new ones; sometimes we quote them. And sometimes we come across a piece of work so elegant and complete that it makes most sense simply to reproduce it whole. (On the Web, we would simply point to it.)

"Law and Borders" is such an essay. It raises and addresses many of the provocative issues of how cyberspace should be governed. Of course, it does not resolve them, but it gives us a way of thinking about them. It is written by lawyers for a general public -- but we wish lawyers and legislators everywhere would read and understand it! Currently, we face a situation where people who don't understand cyberspace are trying to regulate it; that's definitely the wrong sequence.

David Johnson is former chairman of the Electronic Frontier Foundation, among other things. He and David Post now lead the Cyberspace Law Institute, which is tackling some of these issues. Its virtual magistrate recently resolved its first dispute (see page 18).

-- Esther Dyson

Introduction

Global computer-based communications cut across territorial borders, creating a new realm of human activity and undermining the feasibility -- and legitimacy -- of applying laws based on geographic boundaries. While these electronic communications play havoc with geographic boundaries, a new boundary, made up of the screens and passwords that separate the virtual world from the "real world" of atoms, emerges. This new boundary defines a distinct cyberspace →

CYBERSPACE IS A PLACE

<u>INSIDE</u>	
LAW AND BORDERS	1
Territorial borders. Trademarks and more.	
A NEW BOUNDARY	10
Cyberspace as a place. Defamation, fraud and copyright.	
WILL STRUCTURES EMERGE?	17
Trademarks, again.	
RECONCILING CONFLICTS	20
Resist local claims of control.	
INTERNAL DIVERSITY	23
Speciation in cyberspace.	
CONCLUSIONS	28
RESOURCES & CALENDAR	30
Names, phones, dates, URLs.	

that needs and can create new law and legal institutions of its own. Territorially-based law-making and law-enforcing authorities find this new environment deeply threatening. But established territorial authorities may yet learn to defer to the self-regulatory efforts of cyberspace participants who care most deeply about this new digital trade in ideas, information and services. Separated from doctrine tied to territorial jurisdictions, new rules will emerge, in a variety of online spaces, to govern a wide range of new phenomena that have no clear parallel in the nonvirtual world. These new rules will play the role of law by defining legal personhood and property, resolving disputes and crystallizing a collective conversation about core values.

Territorial borders in the "real world"

We take for granted a world in which geographical borders -- lines separating physical spaces -- are of primary importance in determining legal rights and responsibilities: "All law is *prima facie* territorial."¹ Territorial borders, generally speaking, delineate areas within which different sets of legal rules apply. There has until now been a general correspondence between borders drawn in physical space (between nation states or other political entities) and borders in "law space." For example, if we were to superimpose a "law map" (delineating areas where different rules apply to particular behaviors) onto a political map of the world, the two maps would overlap to a significant degree, with clusters of homogenous applicable law and legal institutions fitting within existing physical borders, distinct from neighboring homogenous clusters.

The trademark example

Consider a specific example to which we will refer throughout this article: trademark law -- schemes for the protection of the associations between words or images and particular commercial enterprises. Trademark law is distinctly based on geographical separations. Trademark rights typically arise within a given country, usually on the basis of use of a mark on physical goods or in connection with the provision of services in specific locations within that country. Different countries have different trademark laws, with important differences on matters as central as whether the same name can be used in different lines of business. In the United States, the same name can even be used for the same line of business if there is sufficient geographic separation of use to avoid confusion. In fact, there are many local stores, restaurants and businesses with identical names that do not interfere with each other because their customers do not overlap; Ritz crackers can coexist with the Ritz hotel, the Lutece restaurant with Lutece cosmetics. The physical cues provided by different lines of business allow most marks to be used in multiple lines of commerce without dilution of the other users' rights. There is no global registration scheme. Protection of a particularly famous mark on a global basis requires registration in each country. Trademark owners must not only be constantly alert to territorially-based claims of abandonment and to dilution arising from uses of confusingly similar marks, they must also master the different procedural and jurisdictional laws of various countries that apply in each such instance.

1 *American Banana Co. v. United Fruit Co.* 213 US 347, 357 (1909).

When geographic boundaries for law make sense

Physical borders are not, of course, simply arbitrary creations. Although they may be based on historical accident, geographic borders for law make sense in the real world. Their relationship to the development and enforcement of legal rules is logically based on many related considerations.

Power

Control over physical space, and the people and things located in that space, is a defining attribute of sovereignty and statehood. Law-making requires some mechanism for law enforcement, which in turn depends (to a large extent) on the ability to exercise physical control over, and to impose coercive sanctions on, law-violators. The ability of the sovereign to claim personal jurisdiction over a particular party, for instance, turns importantly on the party's relationship to the physical jurisdiction over which the sovereign has control (e.g., the presence of the party or assets belonging to the party, within the jurisdiction, or activities of the party that are directed to persons or things within the jurisdiction).

Similarly, the law chosen to apply to a contract, tort, or criminal action has historically been influenced primarily by the physical location of the parties or the deed in question. The US government does not impose its trademark law on a Brazilian business operating in Brazil, at least in part because imposing sanctions on the Brazilian business would require assertion of physical control over those responsible for the operation of that business. Such an assertion of control would conflict with the Brazilian government's recognized monopoly on the use of force over its citizens.

Effects

The correspondence between physical boundaries and boundaries in "law space" also reflects a deeply rooted relationship between physical proximity and the effects of any particular behavior. That is, Brazilian trademark law governs the use of marks in Brazil because that use has a more direct impact on persons and assets located within that geographic territory than anywhere else. For example, the existence of a large sign over "Jones' Restaurant" in Rio de Janeiro is unlikely to have an impact on the operation of "Jones' Restaurant" in Oslo, Norway, for we may assume that there is no substantial overlap between the customers, or competitors, of these two entities. Protection of the former's trademark does not -- and probably should not -- affect the protection afforded the latter's.

Legitimacy

We generally accept the notion that the persons within a geographically defined border are the ultimate source of law-making authority for activities within that border. The "consent of the governed" implies that those subject to a set of laws must have a role in their formulation. By virtue of the preceding considerations, the category of persons subject to a sovereign's laws, and most deeply affected by those laws, will consist primarily of individuals who are located in particular physical spaces. Similarly, allocation of responsibility among levels of government proceeds on the assumption that, for many legal problems, physical proximity between the responsible authority and those most directly affected by the law will improve the quality of decision making, and that it is easier to determine the will of those individuals in physical proximity to one another.

Notice

Physical boundaries are also appropriate for the delineation of "law space" in the physical world because they can give notice that the rules change when the boundaries are crossed. Proper boundaries have signposts that provide warning that we will be required, after crossing, to abide by different rules, and physical boundaries -- lines on the geographical map -- are generally well-equipped to serve this signpost function.²

The absence of territorial borders in cyberspace

Cyberspace radically undermines the relationship between legally significant (online) phenomena and physical location. The rise of the global computer network is destroying the link between geographical location and: (1) the power of local governments to assert control over online behavior; (2) the effects of online behavior on individuals or things; (3) the legitimacy of the efforts of a local sovereign to enforce rules applicable to global phenomena; and (4) the ability of physical location to give notice of which sets of rules apply. The Net thus radically subverts a system of rule-making based on borders between physical spaces, at least with respect to the claim that cyberspace should naturally be governed by territorially defined rules.

 "Space is nature's way of keeping everything from happening
 to you."

-- Woody Allen

Cyberspace has no territorially-based boundaries, because the cost and speed of message transmission on the Net is almost entirely independent of physical location: Messages can be transmitted from any physical location to any other location without degradation, decay, or substantial delay, and without any physical cues or barriers that might otherwise keep certain geographically remote places and people separate from one another. The Net enables transactions between people who do not know, and in many cases cannot know, the physical location of the other party. Location remains vitally important, but only location within a virtual space consisting of the "addresses" of the machines between which messages and information are routed. The system is indifferent to the physical location of those machines, and there is no necessary connection between an Internet address and a physical jurisdiction. Although a domain name, when initially assigned to a given machine, may be associated with a particular Internet Protocol address corresponding to the territory within which the machine is physically located (e.g., a

 2 Some "signposts" are culturally understood conventions that accompany entry into specialized places, such as courtrooms, office buildings and churches. But not all signposts and boundaries dividing different rule sets are geographically or physically based. Sets of different rules may apply when the affected parties play particular roles, such as members of self-regulatory organizations, agents of corporate entities and so forth. But even these roles are usually clearly marked by cues of dress, or formal signatures that give warning of the applicable rules. (See Release 1.0, 4-96.)

".uk" domain name extension), the machine may move in physical space without any movement in the logical domain name space of the Net. Or, alternatively, the owner of the domain name might request that the name become associated with an entirely different machine, in a different physical location. Thus, a server with a ".uk" domain name may not necessarily be located in the United Kingdom, a server with a ".com" domain name may be anywhere, and users, generally speaking, are not even aware of the location of the server that stores the content that they read. Physical borders no longer can function as signposts informing individuals of the obligations assumed by entering into a new, legally significant, place, because individuals are unaware of the existence of those borders as they move through virtual space.

Transborder data flow

The power to control activity in cyberspace has only the most tenuous connections to physical location. Many governments first respond to electronic communications crossing their territorial borders by trying to stop or regulate that flow of information as it crosses their borders. Rather than deferring to efforts by participants in online transactions to regulate their own affairs, many governments establish trade barriers, seek to tax any border-crossing cargo, and respond especially sympathetically to claims that information coming into the jurisdiction might prove harmful to local residents. Efforts to stem the flow increase as online information becomes more important to local citizens. In particular, resistance to "transborder data flow" (TDF) reflects the concerns of sovereign nations that the development and use of TDF's will undermine their "informational sovereignty," will negatively impact on the privacy of local citizens, and will upset private property interests in information. Even local governments in the United States have expressed concern about their loss of control over information and transactions flowing across their borders.

But efforts to control the flow of electronic information across physical borders -- to map local regulation and physical boundaries onto cyberspace -- are likely to prove futile, at least in countries that hope to participate in global commerce. Individual electrons can easily, and without any realistic prospect of detection, "enter" any sovereign's territory. The volume of electronic communications crossing territorial boundaries is just too great in relation to the resources available to government authorities to permit meaningful control. US Customs officials have generally given up. They assert jurisdiction over only the physical goods that cross the geographic borders they guard and claim no right to force declarations of the value of materials transmitted by modem. Banking and securities regulators seem likely to lose their battle to impose local regulations on a global financial marketplace. And state Attorneys General face serious challenges in seeking to intercept the electrons that transmit the kinds of consumer fraud that, if conducted physically within the local jurisdiction, would be more easily shut down.

Faced with their inability to control the flow of electrons across physical borders, some authorities strive to inject their boundaries into the new electronic medium through filtering mechanisms and the establishment of electronic barriers. For example, German authorities, seeking to prevent violations of that country's laws against distribution of pornographic material, ordered CompuServe to disable access by German residents to certain global Usenet newsgroups that would otherwise be accessible through that

commercial service. Anyone inside Germany with an Internet connection could, however, easily find a way to access the prohibited news groups during the ban. Although initially compliant, CompuServe subsequently rescinded the ban on most of the files by sending parents a new program to choose for themselves what items to restrict.

Similarly, Tennessee has insisted (indirectly, through enforcement of a federal law that defers to local community standards) that an electronic bulletin board in California install filters that prevent offensive screens from being displayed to users in Tennessee if it is to avoid liability under local obscenity standards in Tennessee. Others have been quick to assert the right to regulate all online trade insofar as it might adversely impact local citizens. The Attorney General of Minnesota, for example, has asserted the right to regulate gambling that occurs on a foreign Web page that was accessed and "brought into" the state by a local resident. The New Jersey securities regulatory agency has similarly asserted the right to shut down any offending Web page accessible from within the state.

Logical roads to virtual places

But such protective schemes will likely fail as well. First, the determined seeker of prohibited communications can simply reconfigure his connection so as to appear to reside in a different location, outside the particular locality, state, or country. Because the Net is engineered to work on the basis of "logical," not geographical, locations, any attempt to defeat the independence of messages from physical locations would be as futile as an effort to tie an atom and a bit together. And, moreover, assertions of law-making authority over Net activities on the ground that those activities constitute "entry into" the physical jurisdiction can just as easily be made by any territorially-based authority. If Minnesota law applies to gambling operations conducted on the World Wide Web because such operations foreseeably affect Minnesota residents, so, too, must the law of any physical jurisdiction from which those operations can be accessed. By asserting a right to regulate whatever its citizens may access on the Net, these local authorities are laying the predicate for an argument that Singapore or Iraq or any other sovereign can regulate the activities of US companies operating in cyberspace from a location physically within the United States. All such Web-based activity, in this view, must be subject simultaneously to the laws of all territorial sovereigns.

Nor are the effects of online activities tied to geographically proximate locations. Information available on the World Wide Web is available simultaneously to anyone with a connection to the global network. The notion that the effects of an activity taking place on that Web site radiate from a physical location over a geographic map in concentric circles of decreasing intensity, however sensible that may be in the nonvirtual world, is incoherent when applied to cyberspace. A Web site physically located in Brazil, to continue with that example, has no more of an effect on individuals in Brazil than does a Web site physically located in Belgium or Belize that is accessible in Brazil. Usenet discussion groups, to take another example, consist of continuously changing collections of messages that are routed from one network to another, with no centralized location at all; they exist, in effect, everywhere, nowhere in particular, and only on the Net.

Nor can the legitimacy of any rules governing online activities be naturally traced to a geographically situated polity. There is no geographically

localized set of constituents with a stronger claim to regulate it than any other local group; the strongest claim to control comes from the participants themselves, and they could be anywhere.

The rise of an electronic medium that disregards geographical boundaries also throws the law into disarray by creating entirely new phenomena that need to become the subject of clear legal rules but that cannot be governed, satisfactorily, by any current territorially-based sovereign. For example, electronic communications create vast new quantities of transactional records and pose serious questions regarding the nature and adequacy of privacy protections. Yet the communications that create these records may pass through or even simultaneously exist in many different territorial jurisdictions. What substantive law should we apply to protect this new, vulnerable body of transactional data? May a French policeman lawfully access the records of communications traveling across the Net from the United States to Japan? Similarly, whether it is permissible for a commercial entity to publish a record of all of any given individual's postings to Usenet newsgroups, or whether it is permissible to implement an interactive Web page application that inspects a user's "bookmarks" to determine which other pages that user has visited, are questions not readily addressed by existing legal regimes -- both because the phenomena are novel and because any given local territorial sovereign cannot readily control the relevant, globally dispersed, actors and actions.³

Because events on the Net occur everywhere but nowhere in particular, are engaged in by online personae who are both "real" (possessing reputations, able to perform services and deploy intellectual assets) and "intangible" (not necessarily or traceably tied to any particular person in the physical sense) and concern "things" (messages, databases, standing relationships) that are not necessarily separated from one another by any physical boundaries, no physical jurisdiction has a more compelling claim than any other to subject these events exclusively to its laws.

The trademark example

The question who should regulate or control Net domain names presents an illustration of the difficulties faced by territorially-based law-making. The

3 Privacy, at least, is a relatively familiar concept, susceptible to definition on the Net by reference to analogies with mail systems, telephone calls and print publication of invasive materials. But many new issues posed by phenomena unique to the Net are not even so familiar. Because electronic communications are not necessarily tied to real world identities, new questions about the rights to continued existence, or to protection of the reputation, of a pseudonym arise. The potential to launch a computer virus or to "spam the net" by sending multiple offpoint messages to newsgroups, for example, creates a need to define rules governing online behavior. When large numbers of people collaborate across the net to create services or works of value, we will face the question whether they have formed a corporate entity or partnership--with rights and duties of its own that are distinct from those of the individual participants--in a context in which there may have been no "registration" with any particular geographic authority and the rights of any such authority to regulate that new "legal person" remain unsettled.

engineers who created the Net devised a "domain name system" that associates numerical machine addresses with easier-to-remember names. Thus, an Internet Protocol machine address such as "36.21.0.69" can be derived, by means of a lookup table, from "leland.stanford.edu." Certain letter extensions (".com," ".edu," ".org," and ".net") have developed as global domains with no association to any particular geographic area. Although the Net creators designed this system as a convenience, it rapidly developed commercial value, because it allows customers to learn and remember the location of particular Web pages or e-mail addresses. Currently, domain names are registered with specific parties who echo the information to "domain name servers" around the world. Registration generally occurs on a "first come, first served" basis,⁴ generating a new type of property akin to trademark rights, but without inherent ties to the trademark law of any individual country. Defining rights in this new, valuable property presents many questions, including those relating to transferability, conditions for ownership (such as payment of registration fees), duration of ownership rights and forfeiture in the event of abandonment, however defined. Who should make these rules?

Consider the placement of a "traditional" trademark on the face of a World Wide Web page. This page can be accessed instantly from any location connected to the Net. It is not clear that any given country's trademark authorities possess, or should possess, jurisdiction over such placements. Otherwise, any use of a trademark on the net would be subject simultaneously to the jurisdiction of every country. Should a Web page advertising a local business in Illinois be deemed to infringe a trademark in Brazil just because the page can be accessed freely from Brazil? Large US companies may be upset by the appearance on the Web of names and symbols that overlap with their valid US-registered trademarks. But these same names and symbols could also be validly registered by another party in Mexico whose "infringing" marks are now, suddenly, accessible from within the United States. Upholding a claim of infringement or dilution launched by the holder of a US-registered trademark, solely on the basis of a conflicting mark on the Net, exposes that same trademark holder to claims from other countries when the use of their US-registered mark on the Web would allegedly infringe a similar mark in those foreign jurisdictions.

Migration of other regulated conduct to the Net

Almost everything involving the transfer of information can be done online: education, health care, banking, the provision of intangible services, all forms of publishing and the practice of law. The laws regulating many of these activities have developed as distinctly local and territorial. Local authorities certify teachers, charter banks with authorized "branches," and license doctors and lawyers. The law has in essence presumed that the activities conducted by these regulated persons cannot be performed without

⁴ Conflicts between domain names and registered trademarks have caused Network Solutions, Inc. (NSI), the agent for registration of domain names in the United States, to require that registrants "represent and warrant" that they have the right to a requested domain name and promise to "defend, indemnify and hold harmless" NSI for any claims stemming from use or registration of the requested name.

being tied to a physical body or building subject to regulation by the territorial sovereign authority, and that the effects of those activities are most distinctly felt in geographically circumscribed areas. These distinctly local regulations cannot be preserved once these activities are conducted by globally dispersed parties through the Net. When many trades can be practiced in a manner that is unrelated to the physical location of the participants, these local regulatory structures will either delay the development of the new medium or, more likely, be superseded by new structures that better fit the online phenomena in question.

Any insistence on "reducing" all online transactions to a legal analysis based in geographic terms presents, in effect, a new "mind-body" problem on a global scale. We know that the activities that have traditionally been the subject of regulation must still be engaged in by real people who are, after all, at distinct physical locations. But the interactions of these people now somehow transcend those physical locations. The Net enables forms of interaction in which the shipment of tangible items across geographic boundaries is irrelevant and in which the location of the participants does not matter. Efforts to determine "where" the events in question occur are decidedly misguided, if not altogether futile.

A NEW BOUNDARY FOR CYBERSPACE

Although geographic boundaries may be irrelevant in defining a legal regime for cyberspace, a more legally significant border for the "law space" of the Net consists of the screens and passwords that separate the tangible from the virtual world. Traditional legal doctrine treats the Net as a mere transmission medium that facilitates the exchange of messages sent from one legally significant geographical location to another, each of which has its own applicable laws. Yet, trying to tie the laws of any particular territorial sovereign to transactions on the Net, or even trying to analyze the legal consequences of Net-based commerce as if each transaction occurred geographically somewhere in particular, is most unsatisfying.

Cyberspace as a place

Many of the jurisdictional and substantive quandaries raised by border-crossing electronic communications could be resolved by one simple principle: conceiving of cyberspace as a distinct "place" for purposes of legal analysis by recognizing a legally significant border between cyberspace and the "real world." Using this new approach, we would no longer ask the unanswerable question "where" in the geographical world a Net-based transaction occurred. Instead, the more salient questions become: What rules are best suited to the often unique characteristics of this new place and the expectations of those who are engaged in various activities there? What mechanisms exist or need to be developed to determine the content of those rules and the mechanisms by which they can be enforced? Answers to these questions will permit the development of rules better suited to the new phenomena in question, more likely to be made by those who understand and participate in those phenomena, and more likely to be enforced by means that the new global communications media make available and effective.

The new boundary is real

Treating cyberspace as a separate "space" to which distinct laws apply should come naturally, because entry into this world of stored online communications occurs through a screen and (usually) a "password" boundary. There is a "placeness" to cyberspace because the messages accessed there are persistent and accessible to many people. You know when you are "there." No one accidentally strays across the border into cyberspace. To be sure, cyberspace is not a homogenous place; groups and activities found at various online locations possess their own unique characteristics and distinctions, and each area will likely develop its own set of distinct rules. But the line that separates online transactions from our dealings in the real world is just as distinct as the physical boundaries between our territorial governments -- perhaps more so.

Crossing into cyberspace is a meaningful act that would make application of a distinct "law of cyberspace" fair to those who pass over the electronic boundary. As noted, a primary function and characteristic of a border or boundary is its ability to be perceived by the one who crosses it. As regulatory structures evolve to govern cyberspace-based transactions, it will be much easier to be certain which of those rules apply to your activities online than to determine which territorial-based authority might apply its laws to your conduct. For example, you would know to abide by the "terms of service" established by CompuServe or America Online when you are

in their online territory, rather than guess whether Germany, or Tennessee, or the SEC will succeed in asserting their right to regulate your activities and those of the "placeless" online personae with whom you communicate.⁵

The trademark example

The ultimate question of who should set the rules for uses of names on the Net presents an apt microcosm for examining the relationship between the Net and territorial-based legal systems. There is nothing more fundamental, legally, than a name or identity: The right to legally recognized personhood is a predicate for the amassing of capital, including the reputational and financial capital, that arises from sustained interactions. The domain name system, and other online uses of names and symbols tied to reputations and virtual locations, exist operationally only on the Net. These names can, of course, be printed on paper or embodied in physical form and shipped across geographic borders. But such physical uses should be distinguished from electronic use of such names in cyberspace, because publishing a name or symbol on the Net is not the same as intentional distribution to any particular jurisdiction. Instead, use of a name or symbol on the Net is like distribution to all jurisdictions simultaneously. Recall that the non-country-specific domain names like ".com," and ".edu" lead to the establishment of online addresses on a global basis. And through such widespread use, the global domain names gained proprietary value. In this context, assertion by any local jurisdiction of the right to set the rules applicable to the "domain name space" is an illegitimate extra-territorial power grab.

Conceiving of the Net as a separate place for purposes of legal analysis will have great simplifying effects. For example, a global registration system for all domain names and reputationally significant names and symbols used on the Net would become possible. Such a Net-based regime could take account of the special claims of owners of strong global marks (as used on physical goods) and "grandfather" these owners' rights to the use of their strong marks in the newly opened online territory. But a Net-based global registration system could also fully account for the true nature of the Net by treating the use of marks on Web pages as a global phenomenon, by assessing the likelihood of confusion and dilution in the online context in which such confusion would actually occur, and by making sure that any rules comply with applicable engineering constraints.

A distinct set of rules applicable to trademarks in cyberspace would greatly simplify matters by providing a basis to resist the inconsistent and conflicting assertions of geographically local prerogatives. If one country objects to the use of a mark on the Web that conflicts with a locally regis-

5 Having a noticeable border may be a prerequisite to the establishment of any legal regime that can claim to be separate from pre-existing regimes. If someone acting in any given space has no warning that the rules have changed, the legitimacy of any attempt to enforce a distinctive system of law is fatally weakened. No geographically based sovereign could plausibly claim to have jurisdiction over a territory with secret boundaries. And no self-regulatory organization could assert its prerogatives while making it hard for members and nonmembers to tell each other apart or disguising when they were (or were not) playing their membership-related roles.

tered mark, the rebuttal would be that the mark has not been used inside the country at all, but only on the Web. If a company wants to know where to register its use of a symbol on the Net, or to check for conflicting prior uses of its mark, the answer will be obvious and cost effective: the designated registration authority for the relevant portion of the Net itself. If we need to develop rules governing abandonment, dilution and conditions on uses of particular types of domain names and addresses, those rules -- applicable specifically to cyberspace -- will be able to reflect the special characteristics of this new electronic medium.

Other cyberspace regimes

Once we take cyberspace seriously as a distinct place for purposes of legal analysis, many opportunities to clarify and simplify the rules applicable to online transactions become available.

Defamation law

Treating messages on the Net as transmissions from one place to another has created a quandary for those concerned about liability for defamation: Messages may be transmitted between countries with very different laws, and liability may be imposed on the basis of "publication" in multiple jurisdictions with varying standards. In contrast, the approach that treats the global network as a separate place would consider any allegedly defamatory message to have been published only "on the Net" (or in some distinct subsidiary area thereof) -- at least until such time as distribution on paper occurs. This re-characterization makes more sense. A person who uploads a potentially defamatory statement would be able more readily to determine the rules applicable to his own actions. Moreover, because the Net has distinct characteristics, including an enhanced ability of the allegedly defamed person to reply, the rules of defamation developed for the Net could take into account these technological capabilities -- perhaps by requiring that the opportunity for reply be taken advantage of in lieu of monetary compensation for certain defamatory net-based messages. The distinct characteristics of the Net could also be taken into account when applying and adapting the "public figure" doctrine in a context that is both global and highly compartmentalized and that blurs the distinction between private and public spaces.

Regulation of Net-based professional activities

The simplifying effect of "taking cyberspace seriously" likewise arises in the context of regimes for regulating professional activities. As noted, traditional regulation insists that each professional be licensed by every territorial jurisdiction where she provides services. This requirement is infeasible when professional services are dispensed over the Net and potentially provided in numerous jurisdictions. Establishing certification regimes that apply only to such activities on the Net would greatly simplify matters. Such regulations would take into account the special features of Net-based professional activities like tele-medicine or global law practice by including the need to avoid any special risks caused by giving online medical advice in the absence of direct physical contact with a patient or by answering a question regarding geographically local law from a remote location. Using this new approach, we could override the efforts of local school boards to license online educational institutions, treating attendance by students at online institutions as a form of "leaving home for school" rather than characterizing the offering of education online as pros-

ecutable distribution of disfavored materials into a potentially unwelcoming community that asserts local licensing authority.

Fraud and antitrust

Even an example that might otherwise be thought to favor the assertion of jurisdiction by a local sovereign -- protection of local citizens from fraud and antitrust violations -- shows the beneficial effects of a cyberspace legal regime. How should we analyze "markets" for antitrust and consumer protection purposes when the companies at issue do business only through the World Wide Web? Cyberspace could be treated as a distinct marketplace for purposes of assessing concentration and market power. Concentration in geographic markets would be relevant only in the rare cases in which such market power could be inappropriately leveraged to obtain power in online markets -- for example by conditioning access to the net by local citizens on their buying services from the same company (such as a phone company) online. Claims regarding a right to access to particular online services, as distinct from claims to access particular physical pipelines, would remain tenuous as long as it is possible to create a new online service instantly in any corner of an expanding online space.

Consumer-protection doctrines could also develop differently online -- to take into account the fact that anyone reading an online ad is only a mouse-click away from guidance from consumer protection agencies and discussions with other consumers. Can Minnesota prohibit the establishment of a Ponzi scheme on a Web page physically based in the Cayman islands but accessed by Minnesota citizens through the Net? Under the proposed new approach to regulation of online activities, the answer is clearly no. Minnesota has no special right to prohibit such activities. The state lacks enforcement power, cannot show specially targeted effects, and does not speak for the community with the most legitimate claim to self-governance. But that does not mean that fraud might not be made "illegal" in at least large areas of cyberspace. Those who establish and use online systems have a interest in preserving the safety of their electronic territory and preventing crime. They are more likely to be able to enforce their own rules. And, as more fully discussed below, insofar as a consensually based "law of the Net" needs to obtain respect and deference from local sovereigns, new Net-based law-making institutions have an incentive to avoid fostering activities that threaten the vital interests of territorial governments.

Copyright law

We suggest, not without some trepidation, that "taking cyberspace seriously" could clarify the current intense debate about how to apply copyright law principles in the digital age. In the absence of global agreement on applicable copyright principles, the jurisdictional problems inherent in any attempt to apply territorially-based copyright regimes to electronic works simultaneously available everywhere on the globe are profound. As Jane Ginsburg has noted:

A key feature of the GII [Global Information Infrastructure] is its ability to render works of authorship pervasively and simultaneously accessible throughout the world. The principle of territoriality becomes problematic if it means that posting a work on the GII calls into play the laws of every country in which the work may be received when...these laws may differ substantively. Should the rights in a work be determined by a multiplicity of inconsistent legal regimes

when the work is simultaneously communicated to scores of countries? Simply taking into account one country's laws, the complexity of placing works in a digital network is already daunting; should the task be further burdened by an obligation to assess the impact of the laws of every country where the work might be received? Put more bluntly, for works on the GII, there will be no physical territoriality.... Without physical territoriality, can legal territoriality persist?⁶

But treating cyberspace as a distinct place for purposes of legal analysis does more than resolve the conflicting claims of different jurisdictions: It also allows the development of new doctrines that take into account the special characteristics of the online "place."

The basic justification for copyright protection is that bestowing an exclusive property right to control the reproduction and distribution of works on authors will increase the supply and diversity of such works by offering authors a financial incentive to engage in the effort required for their creation. But even in the "real world," much creative expression is entirely independent of this incentive structure, because the author's primary reward has more to do with acceptance in a community and the accumulation of reputational capital through wide dissemination than it does with the licensing and sale of individual copies of works; for example, the creative output of lawyers and law professors -- law-review articles, briefs and other pleadings, and the like -- may well be determined largely by factors completely unrelated to the availability or unavailability of copyright protection for those works, because that category of authors, generally speaking, obtains reputational benefits from wide dissemination that far outweigh the benefits that could be obtained from licensing individual copies. And that may be more generally true of authorship in cyberspace; because authors can now, for the first time in history, deliver copies of their creations instantaneously and at virtually no cost anywhere in the world, one might expect authors to devise new modes of operation that take advantage of, rather than work counter to, this fundamental characteristics of the new environment. One such strategy has already begun to emerge: giving away information at no charge -- what might be called the "Netscape strategy" -- as a means of building up reputational capital that can subsequently be converted into income (e.g., by means of the sale of services). As Esther Dyson has written in this newsletter:

Controlling copies (once created by the author or by a third party) becomes a complex challenge. You can either control something very tightly, limiting distribution to a small, trusted group, or you can rest assured that eventually your product will find its way to a large nonpaying audience -- if anyone cares to have it in the first place....

Much chargeable value will be in certification of authenticity and reliability, not in the content. Brand name, identity and other marks of value will be important; so will security of supply. Customers

6 Jane C. Ginsburg, *Global Use/Territorial Rights: Private International Law questions of the Global Information Infrastructure*, *Journal of the Copyright Society*, 1995.

will pay for a stream of information and content from a trusted source. For example, the umbrella of *The New York Times* sanctifies the words of its reporters. The content churned out by *Times* reporters is valuable because the reporters undergo quality-control, and because others believe them....

The trick is to control not the copies of your work but instead a relationship with the customers - subscriptions or membership. And that's often what the customers want, because they see it as an assurance of a continuing supply of reliable, timely content. (Release 1.0, 12-94, as published in *Wired*, August, 1995.)

A profound shift of this kind in regard to authorial incentives fundamentally alters the applicable balance between the costs and benefits of copyright protection in cyberspace, calling for a reappraisal of long-standing principles. So, too, do other unique characteristics of cyberspace severely challenge traditional copyright concepts. For example, consider the very ubiquity of file "copying" -- the fact that one cannot access any information whatsoever in a computer-mediated environment without making a "copy" of that information.⁷

As a consequence, any simple-minded or simplistic attempt to map traditional notions of the author's exclusive rights over the making of "copies" onto cyberspace transactions will likely have perverse results; "if the very act of getting a document to your screen is considered the 'making of a copy' within the meaning of the Copyright Act, then a high proportion of the millions of messages traveling over the Internet each day potentially infringes on the right of some file creator...to control the making of copies. And, if the very act reading such documents on line involves copying, then some form of a license...would, in this view, be required for virtually every one of those message transmissions."⁸ Similarly, application of the "first

7 "For example, 'browsing' on the World Wide Web necessarily involves the creation of numerous 'copies' of information; first, a message is transmitted from Computer A to (remote) Computer B, requesting that Computer B send a copy of a particular file (e.g., the "home page" stored on Computer B) back to Computer A. When the request is received by Computer B, a copy of the requested file is made and transmitted back to Computer A (where it is copied again -- 'loaded' into memory -- and displayed). And the manner in which messages travel across the Internet to reach their intended recipient(s) -- via intermediary computers known as "routers," at each of which the message is 'read' by means of 'copying' the message into the computer's memory -- [involves]...innumerable separate acts of...'reproduction'. File copying is not merely inexpensive in cyberspace, it is ubiquitous; and it is not merely ubiquitous, it is indispensable.... Were you to equip your computer with a 'copy lock' -- an imaginary device that will prevent the reproduction of any and all information now stored in the computer in any form -- it will, essentially, stop functioning." David G. Post, *White Paper Blues: Copyright and the National Information Infrastructure*, Legal Times, April 8, 1996.

8 David G. Post, "New Wine, Old Bottles: The Evanescent Copy," *American Lawyer*, May 1995.

sale" doctrine (allowing the purchaser of a copyrighted work to freely resell the copy she purchased) is problematic when the transfer of a lawfully owned copy technically involves the making of a new copy before the old one is eliminated, as is defining "fair use" when a work's size is indeterminate, ranging from (1) an individual paragraph sold separately on demand in response to searches to (2) the entire database from which the paragraph originates, something never sold as a whole unit.

Treating cyberspace as a distinct location allows for the development of new forms of intellectual property law, applicable only on the Net, that would properly focus attention on these unique characteristics of this new, distinct place while preserving doctrines that apply to works embodied in physical collections (like books) or displayed in legally significant physical places (like theaters). Current debates about applying copyright law to the Net often do, implicitly, treat it as a distinct space, at least insofar as commercial copyright owners somewhat inaccurately refer to it as a "lawless" place. The civility of the debate might improve if everyone assumed the Net should have an appropriately different law, including a special law for unauthorized transfers of works from one realm to the other. We could, in other words, regulate the smuggling of works created in the physical world, by treating the unauthorized uploading of a copy of such works to the Net as infringement.

This new approach would help promoters of electronic commerce focus on developing incentive-producing rules to encourage authorized transfers into cyberspace of works not available now, while also reassuring owners of existing copyrights to valuable works that changes in the copyright law for the Net would not require changing laws applicable to distributing physical works. It would also permit the development of new doctrines of implied license and fair use that, as to works first created on the Net or imported with the author's permission, appropriately allow the transmission and copying necessary to facilitate their use within the electronic realm.⁹

9 For example, we could adopt rules that make the "caching" of web pages presumptively permissible, absent an explicit agreement, rather than adopting the standard copyright doctrine to the contrary (caching involves copying Web pages to a hard drive so that future trips to the site take less time to complete). Because making "cached" copies in computer memory is essential to speed up the operation of the Web, and because respecting express limits or retractions on any implied license allowing caching would clog up the free flow of information, we should adopt a rule favoring browsing.

WILL RESPONSIBLE SELF-REGULATORY STRUCTURES EMERGE ON THE NET?

Even if we agree that new rules should apply to online phenomena, questions remain about who sets the rules and how they are enforced. We believe the Net can develop its own effective legal institutions.

The Trademark Example

In order for the domain name space to be administered by a legal authority that is not territorially based, new law-making institutions will have to develop. Many questions that arise in setting up this system will need answers -- decisions about whether to create a new top level domain, whether online addresses belong to users or service providers and whether one name impermissibly interferes with another, thus confusing the public and diluting the value of the pre-existing name. The new system must also include procedures to give notice in conflicting claims, to resolve these claims and to assess appropriate remedies (including, possibly, compensation) in cases of wrongful use. If the cyberspace equivalent of eminent domain develops, questions may arise over how to compensate individuals when certain domain names are destroyed or redeployed for the public good of the Net community. Someone must also decide threshold membership issues for cyberspace citizens, including how much users must disclose (and to whom) about their real-world identities to use e-mail addresses and domain names for commercial purposes. Implied throughout this discussion is the recognition that these rules will only be meaningful and enforceable if cyberspace citizens view whomever makes these decisions as a legitimate governing body.

Experience suggests that the community of online users and service providers is up to the task of developing a self-governance system. Every system operator who dispenses a password imposes at least some requirements as conditions of continuing access, including paying bills on time or remaining a member of a group entitled to access (e.g. students at a university).¹⁰ System operators (sysops) have an extremely powerful enforcement tool at their disposal to enforce such rules -- banishment. Moreover, communities of users have marshaled plenty of enforcement weapons to induce wrongdoers to comply with local conventions such as rules against flaming, shunning, mailbombs and the like. And both sysops and users have begun explicitly to recognize that formulating and enforcing such rules should be a matter for principled discussion, not an act of will by whoever has control of the power switch.

While many of these new rules and customs apply only to specific, local areas of the global network, some standards apply through technical protocols on a nearly universal basis. And widespread agreement already exists

10 Typical rules also require refraining from actions that threaten the value of the on line space or increase the risk that the system operator will face legal trouble in the real world. Many coherent on line communities also have rules preserving the special character of their on line spaces, rules governing posted messages, discouraging "flaming" (sending an insulting message) or "spamming" (sending the same message to multiple newsgroups), and even rules mandating certain professional qualifications for participants.

about core principles of "netiquette" in mailing lists and discussion groups -- although, admittedly, new users have a slow learning curve and the Net offers little formal "public education" regarding applicable norms. Dispute resolution mechanisms suited to this new environment also seem certain to prosper.¹¹ Cyberspace is anything but anarchic; its distinct rule sets are becoming more robust every day.

Mercantile law

Perhaps the most apt analogy to the rise of a separate law of cyberspace is the origin of the Law Merchant -- a distinct set of rules that developed with the new, rapid boundary-crossing trade of the Middle Ages. Merchants could not resolve their disputes by taking them to the local noble, whose established feudal law mainly concerned land claims. Nor could the local lord easily establish meaningful rules for a sphere of activity he barely understood, executed in locations beyond his control. The result of this jurisdictional confusion, arising from a then-novel form of boundary-crossing communications, was the development of a new legal system -- Lex Mercatoria.

"[D]uring this period, because of the need for uniform laws of commerce to facilitate international trade, '...the basic concepts and institutions of modern Western mercantile law -- lex mercatoria -- were formed, and, even more important, it was then that mercantile law in the West first came to be viewed as an integrated, developing system, a body of law'. Virtually every aspect of commercial transactions in all of Europe (and in cases even outside Europe) were 'governed' by this body of law after the eleventh century. ...This body of law was voluntarily produced, voluntarily adjudicated and voluntarily enforced. In fact, it had to be. There was no other potential source of such law, including state coercion."¹²

The people who cared most about and best understood their new creation formed and championed this new law, which did not destroy or replace existing law regarding more territorially-based transactions (e.g. transferring land ownership). Arguably, exactly the same type of phenomenon is developing in cyberspace right now.

Governments cannot stop electronic communications coming across their borders, even if they want to do so. Nor can they credibly claim a right to regulate the Net based on supposed local harms caused by activities that originate outside their borders and that travel electronically to many different nations; one nation's legal institutions should not, therefore, monopolize rule-making for the entire Net. Even so, established authorities likely will continue to claim that they must analyze and regulate the new online phenomena in terms of some physical locations. After all, the people engaged in online communications still inhabit the material world. And, so

 11 The authors have helped create one such Net-based dispute resolution service, the "Virtual Magistrate;" see <http://vmag.law.vill.edu>.

12 Bruce L. Benson, *The Spontaneous Evolution of Commercial Law*, Southern Economics Journal, 1989.

the argument goes, local legal authorities must have authority to remedy the problems created in the physical world by those acting on the Net. The rise of responsible law-making institutions within cyberspace, however, will weigh heavily against arguments that would claim that the Net is "lawless" and thus tie regulation of online trade to physical jurisdictions. As noted, sysops acting alone or collectively have the power of banishment to control wrongful actions online.

This enforcement tool is not perfect -- any more than the tool of banishing merchants from the medieval trade fairs was perfect for the development of the Law Merchant. Individuals intent on wrongdoing may be able to sneak back on the Net or into a particular online area with a new identity. But the enforcement tools used by legal authorities in the real world also have limits. We do not refrain from recognizing the sovereignty of our territorial governments just because they cannot fully control their physical borders or all of the actions of their citizens. Thus, for online activities that minimally impact the vital interests of sovereigns, the self-regulating structures of cyberspace seem better suited than local authorities to deal with the Net's legal issues.

Editor's note: The many borders in question are moving and blurring. For example, the border between cyberspace and real space may become less evident as the technology blends better into our everyday lives. We may not consider a phone call to be in cyberspace (or in real space), but an audio link over the Internet probably *is* in cyberspace. Connect an Internet phone to an open microphone and multicast what you capture, and you have an unobtrusive, dangerous setup. Similarly, someone could display Web pages in a public area, where passers-by need not log in to see Web content -- a Web billboard. It is likely that these examples will be covered under existing laws regarding taping people without their consent and broadcasting in public spaces.

The borders between different kinds of places in cyberspace are blurring, too, and in ways more difficult to resolve. Today, the Internet and commercial online services look quite different from each other. You definitely know when you're logging into Prodigy, for example. But the commercial services are moving quickly to the Web. They are adding similar kinds of features and functions. Soon they will look far more like each other -- and like any other Website -- than before. The only artifact that will indicate entry into a different space will be the login screen. Yet that login screen is itself in danger of vanishing: apply Apple's "keychain" function to any subscription site, and you only use your password once -- when you start using your computer. (This is a good thing for usability, though it is probably unfortunate insofar as border markings are concerned).

Software and service designers need to fill the gap by creating -- and helping everyone agree on -- affordances that everyone can learn. Think of them as the "stop" and "yield" signs of cyberspace, but with new content. The signs might indicate that the spaces they delimit contain adult content, require occupants to identify themselves fully and truthfully, or are subject to New York State law and taxes.

LOCAL AUTHORITIES, FOREIGN RULES: RECONCILING CONFLICTS

What should happen when conflicts arise between the local territorial law (applicable to persons or entities by virtue of their location in a particular area of physical space) and the law applicable to particular activities on the Net? The doctrine of "comity," as well as principles applied when delegating authority to self-regulatory organizations, provide us with guidance for reconciling such disputes.

The doctrine of comity, in the Supreme Court's classic formulation, is "the recognition which one nation allows within its territory to the legislative, executive, or judicial acts of another nation, having due regard both to international duty and convenience and to the rights of its own citizens or of other persons who are under the protections of its law." It arose as an attempt to mitigate some of the harsher features of a world in which lawmaking is an attribute of control over physical space but in which persons, things and actions may move across physical boundaries, and it functions as a constraint on the strict application of territorial principles that attempts to reconcile "the principle of absolute territorial sovereignty [with] the fact that intercourse between nations often demand[s] the recognition of one sovereign's lawmaking acts in the forum of another."

In general, comity reflects the view that those who care more deeply about and better understand the disputed activity should determine the outcome. Accordingly, it may be ideally suited to handle, by extension, the new conflicts between the a-territorial nature of cyberspace activities and the legitimate needs of territorial sovereigns and of those whose interests they protect on the other side of the cyberspace border. This doctrine does not disable territorial sovereigns from protecting the interests of those individuals located within their spheres of control, but it calls upon them to exercise a significant degree of restraint when doing so.

Faith as an online experience

Local officials handling conflicts can also learn from the many examples of delegating authority to self-regulatory organizations. Churches are allowed to make religious law.¹³ Clubs and social organizations can, within broad limits, define rules that govern activities within their spheres of interest. Securities exchanges can establish commercial rules, so long as they protect the vital interests of the surrounding communities. In these cases, government has seen the wisdom of allocating rule-making functions to those who best understand a complex phenomenon and who have an interest in assuring the growth and health of their shared enterprise.

Cyberspace represents a new permutation of the underlying issue: How much local authorities should defer to a new, self-regulating activity arising

13 "Of course, the primitive Church was a kind of Internet itself, which was one of the reasons it was so difficult for the Roman Empire to combat it. The early Christians understood that what was most important was not to claim physical power in a physical place but to establish a network of believers -- to be on line," *The Virtual Bishop*, by Adam Gopnik; *New Yorker*, March 18, 1996; quoting French Bishop Jacques Gaillot.

independently of local control and reaching beyond the limited physical boundaries of the sovereign. This mixing of both tangible and intangible boundaries leads to a convergence of the intellectual categories of comity in international relations and the local delegation by a sovereign to self-regulatory groups. In applying both the doctrine of "comity" and the idea of "delegation" to cyberspace, a local sovereign is called upon to defer to the self-regulatory judgments of a population that can easily include people outside its physical jurisdiction.

Despite the seeming contradiction of a sovereign deferring to the authority of those who are not its own subjects, such a policy makes sense, especially in light of the underlying purposes of both doctrines. Comity and delegation represent the wise conservation of governmental resources and allocate decisions to those who most fully understand the special needs and characteristics of a particular "sphere" of being. Although cyberspace represents a new sphere that cuts across national boundaries, the fundamental principle remains. If the sysops and users who collectively inhabit and control a particular area of the Net want to establish special rules to govern conduct there, and if that rule set does not fundamentally impinge upon the vital interests of others who never visit this new space, then the law of sovereigns in the physical world should defer to this new form of self-government.

The trademark perspective

Consider, once again, the trademark example. A US government representative has stated that, since the government paid for the initial development and administration of the domain name system, it "owns" the right to control policy decisions regarding the creation and use of such names. Obviously, government funds, in addition to individual efforts on a global scale, created this valuable and finite new asset. But the government's claim based on its investment is not particularly convincing. In fact, the United States may be asserting its right to control the policies governing the domain name space primarily because it fears that any other authority over the Net might force it to pay again for the ".gov" and ".mil" domain names used by governmental entities.

To assuage these concerns, a Net-based authority should concede to the governments on this point. For example, it should accommodate the military's strong interest in remaining free to regulate and use its ".mil" addresses. A new Net-based standards-making authority should also accommodate the government's interests in retaining its own untaxed domain names and other issues with direct impact on the government's operation. Given responsible restraint by the Net-based authority and the development of an effective self-regulatory scheme, the government might well then decide that it should not spend its finite resources trying to wrest effective control of non-governmental domain names away from those who care most about facilitating the growth of online trade.

Because controlling the flow of electrons across physical boundaries is so difficult, a local jurisdiction that seeks to prevent its citizens from accessing specific materials must either outlaw all access to the Net -- thereby cutting itself off from the new global trade -- or seek to impose its will on the Net as a whole. This would be the modern equivalent of a local lord in medieval times either trying to prevent the silk trade from

passing through his boundaries (to the dismay of local customers and merchants) or purporting to assert jurisdiction over the known world. It may be most difficult to envision local territorial sovereigns deferring to the law of the Net when the perceived threat to local interests arises from the very free flow of information that is the Net's most fundamental characteristic -- when, for example, local sovereigns assert an interest in seeing that their citizens are not adversely affected by information that the local jurisdiction deems harmful but that is freely (and lawfully) available elsewhere, such as the incidents mentioned earlier involving the German government's attempts to prevent its citizens access to prohibited materials and the prosecution of a California bulletin board operator for making material offensive to local "community standards" available for downloading in Tennessee. Local sovereigns may insist that their interest (in protecting their citizens from harm) is paramount and easily outweighs any purported interest in making this kind of material freely available. But the opposing interest is not simply the interest in seeing that individuals have access to ostensibly obscene material, it is the "meta-interest" of Net citizens in preserving the global free flow of information.

Local claims of control

If there is one central principle on which all local authorities within the Net should agree, it must be that territorially local claims to restrict online transactions (in ways unrelated to vital and localized interests of a territorial government) should be resisted. This is the Net equivalent of the First Amendment, a principle already recognized in the form of the international human rights doctrine protecting the right to communicate. Participants in the new online trade must oppose external regulation designed to obstruct this flow.

This naturally central principle of online law bears importantly on the "comity" analysis, because it makes clear that the need to preserve a free flow of information across the Net is just as vital to the interests of the Net as the need to protect local citizens against the impacts of unwelcome information may appear from the perspective of a local territorial sovereign. Moreover, the right of individuals to participate in various online realms depends critically on their obtaining information about those realms. Insofar as any territorial government merely claims moral superiority of its laws and values, it is not well situated to oppose a free flow of information that might lead its citizens to disagree, for this would be the equivalent of defending ignorance as a necessary ingredient of preservation of the values espoused by the local state. This view is unlikely to persuade external rulemakers who do not share those values. For the Net to realize its full promise, online rule-making authorities must not respect the claims of territorial sovereigns to restrict online communications when unrelated to vital and localized governmental interests.

INTERNAL DIVERSITY

One of a border's key characteristics is that it slows the interchange of people, things and information across its divide. Arguably, distinct sets of legal rules can only develop and persist where effective boundaries exist. The development of a true "law of cyberspace," therefore, depends upon a dividing line between this new online territory and the nonvirtual world. Our argument so far has been that the new sphere online is cut off, at least to some extent, from rule-making institutions in the material world and requires the creation of a distinct law applicable just to the online sphere.

But we hasten to add that cyberspace is not, behind that border, a homogeneous or uniform territory, where information flows without further impediment. Although it is meaningless to speak of a French or Armenian portion of cyberspace, because the physical borders dividing French or Armenian territory from their neighbors cannot generally be mapped onto the flow of information in cyberspace, the Net has other kinds of internal borders delineating many distinct internal locations that slow or block the flow of information. Distinct names and (virtual) addresses, special passwords, entry fees and visual cues -- software boundaries -- can distinguish subsidiary areas from one another.

The Usenet newsgroup "alt.religion.scientology" is distinct from "alt.misc.legal," each of which is distinct from a chat room on CompuServe or America Online which, in turn, are distinct from the Cyberspace Law Institute listserver or Counsel Connect. Users can only access these different forums through distinct addresses or phone numbers, often navigating through login screens, the use of passwords, or the payment of fees. Indeed, the ease with which internal borders, consisting entirely of software protocols, can be constructed is one of cyberspace's most remarkable and salient characteristics. Electronic mailing lists, for example, can be set up on any network (or Internet) server by means of simple instructions given to one of several widely-available software programs (e.g., listserv, listproc or majordomo). A Usenet discussion group in the "alt." hierarchy can be established by sending a simple request to the "alt.config" newsgroup.

Cyberspace not only permits the effective delineation of internal boundaries between different online spaces, but it also allows for effective delineation of distinct online roles within different spheres of activity and as to which different rules apply. In the nonvirtual world, we slip in and out of such roles frequently; the rules applicable to the behavior of a single individual, in a single territorial jurisdiction, may change as he moves between different legally significant personae (acting as an employee, a member of a church, a parent, or the officer of a corporation, for example). Cyberspace may make the boundaries between these different roles easier to maintain, insofar as explicit "tags" -- distinct "signature files," or screen names -- can relatively easily be attached to messages originating from the author's different roles.

Speciation in cyberspace

The separation of subsidiary "territories" or spheres of activity within cyberspace and the barriers to exchanging information across these internal borders allow for the development of distinct rule sets and for the divergence of those rule sets over time. The processes underlying biological

evolution provide a useful analogy. Speciation -- the emergence over time of multiple, distinct constellations of genetic information from a single, original group -- cannot occur when the original population freely exchanges information (in the form of genetic material) among its members. In other words, a single, freely-interbreeding population of organisms cannot divide into genetically distinct populations; while the genetic material in the population changes over time, it does so more or less uniformly (e.g. the population of the species *Homo erectus* becomes a population of *Homo sapiens*) and cannot give rise to more than one contemporaneous, distinct genetic set.

Speciation requires, at a minimum, some barrier to the interchange of genetic material between subsets of the original homogeneous population. Ordinarily, a physical barrier suffices to prevent one subgroup from exchanging genetic data with another. Once this "border" is in place, divergence within the "gene pool" -- the aggregate of the underlying genetic information -- in each of the two subpopulations can occur. Over time, this divergence may be substantial enough that even when the physical barrier disappears, the two subgroups can no longer exchange genetic material -- that is, they have become separate species.

Software worlds

Rules, like genetic material, are self-replicating information. The internal borders within cyberspace will thus allow for differentiation among distinct constellations of such information -- in this case rule-sets rather than species. Content or conduct acceptable in one "area" of the Net may be banned in another. Institutions that resolve disputes in one "area" of cyberspace may not gain support or legitimacy in others. Local sysops can, by contract, impose differing default rules regarding who has the right, under certain conditions, to replicate and redistribute materials that originate with others. And while cyberspace's reliance on bits instead of atoms may make physical boundaries more permeable, the boundaries delineating digital online "spheres of being" may become less permeable. Cyberspace, as Ethan Katsh has written, is a "software world" where "code is the Law."

"To a considerable extent, networks really are what software allows them to be. The Internet is not a network but a set of communications protocols. ...[T]he Internet is software. Similarly, the World Wide Web is not anything tangible. It is client-server software that permits machines linked on a network to share and work with information on any of the connected machines."¹⁴

And software specifications can be unforgiving (as anyone who has tried to send an e-mail message to an incorrectly spelled network recipient can attest):

Entry of messages into, and routing of messages across, digitally-based electronic networks...are controlled by more effective protocols [than generally govern non-electronic communications networks in the

14 M. Ethan Katsh, *Software Worlds and the First Amendment: Virtual Doorkeepers in Cyberspace*, Univ. of Chicago Legal Forum (forthcoming), quoting William Mitchell, *City of Bits* (MIT Press, 1995).

"real world"]]: each network's technical specifications (typically embodied in software or switching mechanisms) constitute rules that precisely distinguish between compliant and non-compliant messages. This boundary [is not an] artificial construct because the rules are effectively self-enforcing. To put the matter simply, you can't 'almost' be on the Georgetown University LAN or America Online -- you are either transmitting LAN- or AOL-compliant messages or you are not."¹⁵

Thus, individual network communities can be configured, by means of unique specifications of this kind, to bar all (or some specified portion of) inter-network traffic with relative ease, and securing online systems from unauthorized intruders may prove an easier task than sealing physical borders from unwanted immigration. Groups can establish online corporate entities or membership clubs that tightly control participation in, or even public knowledge of, their own affairs. Such groups can reach agreement on or modify these rules more rapidly via online communications. Accordingly, the rule sets applicable to the online world may quickly evolve away from those applicable to more traditional spheres and develop greater variation among the sets.

Developing a civic voice

How this process of differentiation and evolution will proceed is one of the more complex and fascinating questions about law in cyberspace -- and a subject beyond the scope of this article. We should point out, however, an important normative dimension to the proliferation of these internal boundaries between distinct communities and distinct rule-sets and the process by which law will evolve in cyberspace. Cyberspace may be an important forum for the development of new connections between individuals and mechanisms of self-governance by which individuals attain an increasingly elusive sense of community (see **Release 1.0**, 6-93 and 7-93). Commenting on the erosion of national sovereignty in the modern world and the failure of the existing system of nation-states to cultivate a "civic voice," a moral connection between the individual and the community (or communities) in which she is embedded, Michael Sandel has written:

"The hope for self-government today lies not in relocating sovereignty but in dispersing it. The most promising alternative to the sovereign state is not a cosmopolitan community based on the solidarity of humankind but a *multiplicity of communities and political bodies* -- some more extensive than nations and some less -- among which sovereignty is diffused. Only a politics that disperses sovereignty both upward [to transnational institutions] and downward can combine the power required to rival global market forces with the differentiation required of a public life that hopes to inspire the allegiance of its citizens. ...If the nation cannot summon more than a minimal commonality, it is unlikely that the global community can do better, at least on its own. A more promising basis for a democratic politics that reaches beyond nations is a revitalized civic life nourished in the more particular

 15 David G. Post, *Anarchy, State, and the Internet: An Essay on Law-Making in Cyberspace*, 1995; *Journal of Online Law*, available at www.law.cornell.edu/jol/jol.table.html.

communities we inhabit. In the age of NAFTA the politics of neighborhood matters more, not less."¹⁶

Furthermore, the ease with which individuals can move between different rule sets in cyberspace has important implications for any contract-based political philosophy deriving a justification of the State's exercise of coercive power over its citizens from their consent to the exercise of that power. In the nonvirtual world, this consent has a strong fictional element:

State reliance on consent inferred from someone merely remaining in the state is particularly unrealistic. An individual's unwillingness to incur the extraordinary costs of leaving his or her birthplace should not be treated as a consensual undertaking to obey state authority.¹⁷

To be sure, citizens of France, dissatisfied with French law and preferring, say, Armenian rules, can try to persuade their compatriots and local decision-makers of the superiority of the Armenian rule-set. In Hirschman's terms, they have a "voice" in the development of French law, at least to the extent that French law-making institutions represent and are affected by citizen participation, but their "exit" option is limited by the need to physically relocate to Armenia to take advantage of that rule set. In contrast, in cyberspace, any given user has a more accessible exit option, in terms of moving from one virtual environment's rule set to another's, thus providing a more legitimate "selection mechanism" by which differing rule sets will evolve over time.

Optimal production of laws?

The ease with which individuals may move between communities (or inhabit multiple communities simultaneously through a fractionation of their own individual identities) also implies that cyberspace may provide conditions necessary and sufficient for something more closely resembling the optimal collective production of a particular set of goods -- namely, "laws" -- than can be achieved in the real world. Cyberspace may closely approximate Tiebout's idealized model for the allocation of local goods and services, in which optimal allocation of locally-produced public goods is provided by small jurisdictions competing for mobile residents. The Tiebout model of intergovernmental competition has four components: (1) a perfectly elastic supply of jurisdictions, (2) costless mobility of individuals among jurisdictions, (3) full information about the attributes of all jurisdictions and (4) no interjurisdictional externalities. In a Tieboutian world,

...each locality provides a package of local public goods consistent with the preferences of its residents (consumer-voters). Residents whose preferences remain unsatisfied by a particular locality's package of goods and services would (costlessly) move....Escape from un-

16 Michael Sandel, *America's Search for a New Public Philosophy*, *Atlantic Monthly*, March 1996 (emphasis added).

17 Lea Brilmayer, *Consent, Contract, and Territory*, *Minnesota Law Review*, 1975.

desirable packages of goods and services is feasible as a result of two explicit characteristics of the Tiebout model: absence of externalities and mobility of residents.¹⁸

We suggest that cyberspace may be a closer approximation to ideal Tieboutian competition between rule-sets than exists in the nonvirtual world, a consequence of (1) the low cost of establishing an online "jurisdiction," (2) the ease of exit from online communities, (3) the relative ease of acquiring information about the practices of online communities and (4) the greater impermeability of the internal, software-mediated boundaries between online communities in cyberspace, which may mitigate (at least to some extent) the problem of inter-community externalities.

Frequent switching

The ability of inhabitants of cyberspace to cross borders at will between legally significant territories, many times in a single day, is unsettling. This power seems to undercut the validity of developing distinct laws for online culture and commerce: How can these rules be "law" if participants can literally turn them on and off with a switch? Frequent online travel might subject relatively mobile human beings to a far larger number of rule sets than they would encounter traveling through the physical world over the same period. Established authorities, contemplating the rise of a new law applicable to online activities, might object that we cannot easily live in a world with too many different sources and types of law, particularly those made by private (non-governmental) parties, without breeding confusion and allowing anti-social actors to escape effective regulation.

But the speed with which we can cross legally meaningful borders or adopt and then shed legally significant roles should not reduce our willingness to recognize multiple rule sets. Rapid travel between spheres of being does not detract from the distinctiveness of the boundaries, as long as participants realize the rules are changing. Nor does it detract from the appropriateness of rules applying within any given place, any more than changing commercial or organizational roles in the physical world detracts from a person's ability to obey and distinguish rules as a member of many different institutional affiliations and to know which rules are appropriate for which roles. Nor does it lower the enforceability of any given rule set within its appropriate boundaries, as long as groups can control unauthorized boundary crossing of groups or messages.

Alternating between different legal identities many times during a day may confuse those for whom cyberspace remains alien territory, but for those for whom cyberspace is a more natural habitat it may become second nature. Legal systems must learn to accommodate a more mobile kind of legal person. As Sandel has written, "Self-government today...requires a politics that plays itself out in a multiplicity of settings, from neighborhoods to nations to the world as a whole. Such a politics requires citizens who can abide the ambiguity associated with divided sovereignty, who can think and act as multiply situated selves."

18 Gillette, *In Partial Praise of Dillon's Rule, or, Can Public Choice Theory Justify Local Government Law*, *Chi-Kent Law Review* (1991).

CONCLUSION

Global electronic communications have created new spaces in which distinct rule sets will evolve. We can reconcile the new law created in this space with current territorially-based legal systems by treating it as a distinct doctrine, applicable to a clearly demarcated sphere, created primarily by legitimate, self-regulatory processes, and entitled to appropriate deference -- but also subject to limitations when it oversteps its appropriate sphere.

The law of any given place must take into account the special characteristics of the space it regulates and the types of persons, places and things found there. Just as a country's jurisprudence reflects its unique historical experience and culture, the law of cyberspace will reflect its special character, which differs markedly from anything found in the physical world. For example, the law of the Net must deal with persons who "exist" in cyberspace only in the form of an email address and whose purported identity may or may not accurately correspond to physical characteristics in the real world. In fact, an e-mail address might not even belong to a single person. Accordingly, if cyberspace law is to recognize the nature of its "subjects," it cannot rest on the same doctrines that give geographically based sovereigns jurisdiction over "whole," locatable, physical persons. The law of the Net must be prepared to deal with persons who manifest themselves only by means of a particular ID, user account, or domain name.

Moreover, if rights and duties attach to an account itself, rather than an underlying real-world person, traditional concepts such as "equality," "discrimination," or even "rights and duties" may not work as we normally understand them. New angles on these ideas may develop. For example, when AOL users joined the Net in large numbers, other cyberspace users often ridiculed them based on the "@aol.com" tag on their email addresses -- a form of "domainism" that might be discouraged by new forms of netiquette. If a doctrine of cyberspace law accords rights to users, we will need to decide whether those rights adhere only to particular types of online appearances, as distinct from attaching to particular individuals in the real world.

Units that matter

Similarly, the types of "properties" that can become the subject of legal discussion in cyberspace will differ from real-world real estate or tangible objects. For example, in the real world the physical covers of a book delineate the boundaries of a "work" for purposes of copyright law; those limits may disappear entirely when the same materials are part of a large electronic database. Thus, we may have to change the "fair use" doctrine in copyright law that previously depended on calculating what portion of the physical work was copied. Similarly, a Web page's "location" in cyberspace may take on a value unrelated to the physical place where the disk holding that Web page resides, and efforts to regulate Web pages by attempting to control physical objects may only cause the relevant bits to move from one place to another. On the other hand, the boundaries set by "URLs" (Uniform Resource Locators, the location of a document on the World Wide Web) may need special protection against confiscation or confusingly similar addresses. And, because these online "places" may contain offensive material, we may need rules requiring (or allowing) groups to post certain signs or markings at these places' outer borders.

The boundaries that separate persons and things behave differently in the virtual world but are nonetheless legally significant. Messages posted under one e-mail name will not affect the reputation of another e-mail address, even if the same physical person authors both messages. Materials separated by a password will be accessible to different sets of users, even if those materials physically exist on the very same hard drive. A user's claim to a right to a particular online identity or to redress when that identity's reputation suffers harm, may be valid even if that identity does not correspond exactly to that of any single person in the real world.

Clear boundaries make law possible, encouraging rapid differentiation between rule sets and defining the subjects of legal discussion. New abilities to travel or exchange information rapidly across old borders may change the legal frame of reference and require fundamental changes in legal institutions. Fundamental activities of lawmaking -- accommodating conflicting claims, defining property rights, establishing rules to guide conduct, enforcing those rules and resolving disputes -- remain very much alive within the newly defined, intangible territory of cyberspace. At the same time, the newly emerging law challenges the core idea of a current law-making authority -- the territorial nation state, with substantial but legally restrained powers.

If the rules of cyberspace thus emerge from consensually based rule sets, and the subjects of such laws remain free to move among many differing online spaces, then considering the actions of cyberspace's system administrators as the exercise of a power akin to "sovereignty" may be inappropriate. Under a legal framework where the top level imposes physical order on those below it and depends for its continued effectiveness on the inability of its citizens to fight back or leave the territory, the legal and political doctrines we have evolved over the centuries are essential to constrain such power. In that situation, where exit is impossible, costly or painful, then a right to a voice for the people is essential. But when the "persons" in question are not whole people, when their "property" is intangible and portable, and when all concerned may readily escape a jurisdiction they do not find empowering, the relationship between the "citizen" and the "state" changes radically. Law, defined as a thoughtful group conversation about core values, will persist. But it will not, could not and should not be the same law as that applicable to physical, geographically-defined territories.

COMING SOON

- *Industry strategy and dynamics.*
- *Collaboration and conversation tools.*
- *Networked object graphics.*
- *And much more... (If you know of any good examples of the categories listed above, please let us know.)*

RESOURCES & PHONE NUMBERS

David R. Johnson is chairman of Counsel Connect and Co-Director of the Cyberspace Law Institute. He can be reached at (202) 496-9523; fax, (202) 496-9266; david.johnson@counsel.com.

David G. Post is Visiting Associate Professor of Law, Georgetown University Law Center and Co-Director of the Cyberspace Law Institute. He can be reached at (202) 364-5010; david.post@counsel.com.

A version of this paper was presented at a symposium on "Law and Borders" at the Stanford Law School on February 24, 1996, and will appear in a future issue of the Stanford Law Review. The paper was edited for this newsletter. It is available in full text on the Web at www.cli.org/X00025_LBFIN.html. The authors wish to thank Becky Burr, Larry Downes, Henry J. Perritt, Jr. and Ron Plessner, as well as the other Fellows of the Cyberspace Law Institute (Jerry Berman, John Brown, Bill Burrington, Esther Dyson, David Farber, Ken Freeling, A. Michael Froomkin, Robert Gellman, I. Trotter Hardy, Ethan Katsh, Lawrence Lessig, Bill Marmon, Lance Rose, Marc Rotenberg, Pamela Samuelson and Eugene Volokh), CLI Co-Directors Carey Heckman, John Podesta, Peggy Radin and Jim Campbell, for their assistance in the formulation of these ideas. The usual disclaimer, of course, applies: the authors alone are responsible for errors, omissions, misstatements and misunderstandings set forth in the text.

Release 1.0 is published monthly, except for a combined July/August issue, by EDventure Holdings, 104 Fifth Ave., New York, NY 10011-6901; (212) 924-8800; fax, (212) 924-0240. It covers PCs, software, the Internet, computer-telephone integration, online services, groupware, text management, connectivity, messaging, wireless communications, intellectual property law and other unpredictable topics. Editor: Esther Dyson (edyson@edventure.com); publisher: Daphne Kis (daphne@edventure.com); managing editor: Jerry Michalski (spiff@edventure.com); circulation & fulfillment manager: Robyn Sturm (robyn@edventure.com); administrative assistant: Susanna Stromberg (susanna@edventure.com); executive assistant: Christy Snipp (christy@edventure.com); editorial & marketing communications consultant: William M. Kutik (kutik@edventure.com). Copyright 1996, David R. Johnson and David G. Post. All rights reserved. No material in this publication may be reproduced without written permission; however, we gladly arrange for reprints or bulk purchases. Subscriptions cost \$595 per year, \$650 overseas.

RELEASE 1.0 CALENDAR

- June 24-26** **Intr@net '96** - San Jose, CA. Sponsored by Computerworld. Targeted to senior IT execs. Call Stuart Dale, (800) 340-2366; fax (508) 620-9430; stuart_dale@cw.com.
- July 10-12** **WCA '96** - Denver. Sponsored by the Wireless Cable Association. Can wireless cable bypass the phone and terrestrial cable companies? Call Connie Clark, (202) 452-7823; fax (202) 452-0041; www.cais.com/wca/wca96.html.
- July 21-24** **Interactive Services Association 11th Annual Conference** - San Diego. Sponsored by the ISA. With AT&T's John Petrillo. Call Patti McKnight, (301) 495-4955; fax (301) 495-4959; isa@isa.net; www.isa.net.
- July 28-30** **Spotlight** - Laguna Niguel, CA. Hosted by Spotlight. With Red Burns, Lisa Gansky and Norman Perlstine. Call Denise Caruso, (415) 312-0545; fax (415) 286-2750; dcaruso@aol.com.
- July 25-26** **New Media Hollywood** - Santa Monica, CA. Organized by World Research Group. Ad agencies and creative teams meet Web people. Call (800) 647-7600 or (212) 421-9410; fax (212) 421-7325; info@worldrg.com; www.inter.net/wrg/.
- July 28-31** **Genetic Programming '96** - Stanford, CA. Sponsored by Stanford University, the ACM, IEEE and AAAI. Call (415) 328-3123; fax (415) 321-4457; gp@aaai.org; www.cs.brandeis.edu/-zipper/gp-96.html.
- July 31 - Aug 2** **@Web Interactive '96** - New York City. Produced by Meckler-media. With Martin Nisenholtz, Mark Pesce and Jack Hidary; covering graphics, programming and streaming media on the Web. Call (800) MECKLER or (203) 226-6967; fax (203) 226-6976; webint@mecklermedia.com; events.iworld.com/summer96/webint (secure Web server).
- August 4-9** **@SIGGRAPH '96** - New Orleans, LA. Hosted by ACM/SIGGRAPH. Call (312) 321-6830; fax (312) 321-6876; siggraph96@siggraph.org; www.siggraph.org/conferences/siggraph96/core/index.html.
- October 27-29** ****EDventure's High-Tech Forum** - Lisbon, Portugal. Sponsored by EDventure Holdings. Call Daphne Kis, (212) 924-8800; fax (212) 924-0240; daphne@edventure.com.

1997

- March 23-26** ****PC (Platforms for Communication) Forum** - Tucson, AZ. Sponsored by us: You read the newsletter; now meet the players. Call Daphne Kis, (212) 924-8800; fax (212) 924-0240; daphne@edventure.com; www.edventure.com.

* Events Esther plans to attend.

@ Events Jerry plans to attend.

Lack of a symbol is no indication of lack of merit.

The full, current calendar is available on our Website (www.edventure.com).

Please let us know about other events we should include. -- Susanna Stromberg

RELEASE 1.0

SUBSCRIPTION FORM

Please enter my subscription to **Release 1.0** at the rate of \$595 per year in the U.S. and Canada. Overseas subscriptions are \$650, airmail postage included. Payment must be enclosed. Multiple-copy rates available on request. Satisfaction guaranteed or your money back.

Name _____

Title _____

Company _____

Address _____

City _____ State _____ Zip _____

Telephone _____

☐ Check enclosed.

☐ Charge my

☐ American Express ☐ MasterCard ☐ Visa

Card Number _____ Expiration Date _____

Name on Card _____ Signature _____

☐ Please send me information on your multiple-copy rate.

Please fill in the information above and send to:

EDVENTURE HOLDINGS INC.
104 FIFTH AVENUE, 20TH FLOOR
NEW YORK, NY 10011

If you have any questions, please call us at 1 (212) 924-8800;
Fax 1 (212) 924-0240; e-mail info@edventure.com.

Daphne Kis
Publisher